(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－36023
(P2003－36023A)
(43)公開日　平成15年２月７日(2003.2.7)

(51)Int.Cl.[7]	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ　５Ｊ１０４

審査請求　未請求　請求項の数７　ＯＬ　（全 12 頁）

(21)出願番号　特願2001－224890(P2001－224890)

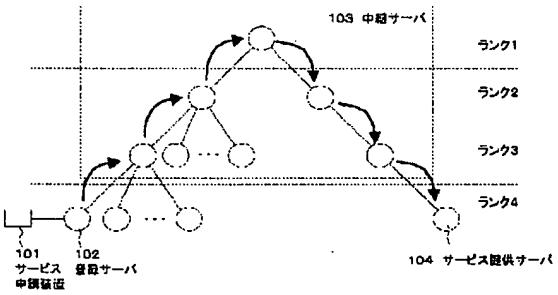
(22)出願日　平成13年７月25日(2001.7.25)

(71)出願人　000222174
東洋エンジニアリング株式会社
東京都千代田区霞が関３丁目２番５号
(72)発明者　前田　陽造
千葉県千葉市若葉区千城台東２－39－１
ダイアパレス千城台ＩＩ　1107
(72)発明者　桑田　博
千葉県千葉市若葉区小倉町1762
(74)代理人　100110928
弁理士　速水　進治　（外１名）

Ｆターム(参考)　5J104 AA09 LA03 LA05 NA02 PA07

(54)【発明の名称】　ネットワークシステムおよびそれを用いた情報送信方法

(57)【要約】
【課題】　電子署名を用いたネットワーク上の情報送信において、管理する鍵の数を低減しつつ、高いセキュリティレベルを実現し、なりすましや改ざん等の不正行為を効果的に防止する技術を提供する。
【解決手段】　複数の情報処理装置がツリー状に配列されたネットワークシステムを用い、サービス申請装置１０１から登録サーバ１０２を経てサービス提供サーバ１０４へメッセージを送信する。ネットワークを構成する各情報処理装置間において、送信元情報処理装置は、送信元情報処理装置固有の秘密鍵により作成した電子署名を付加した状態でメッセージを送信し、送信先情報処理装置は、送信元情報処理装置の公開鍵を用いて前記電子署名を復号化することによりメッセージを検証する。



1

【特許請求の範囲】

【請求項１】　複数の情報処理装置がツリー状に配列された階層構造を有し、該階層構造中の第一の情報処理装置がユーザから受け付けたメッセージを、相互接続された情報処理装置間のパスを一または二以上経由させて、前記メッセージに応答する前記階層構造中の第二の情報処理装置へ送信するネットワークシステムであって、各情報処理装置は、その装置固有の秘密鍵を有し、その装置と直接接続する他の情報処理装置は、前記秘密鍵に対応する公開鍵を有し、相互接続された情報処理装置間のパスにおいてメッセージが送信される際、送信元情報処理装置は、送信元情報処理装置固有の秘密鍵により作成した電子署名を付加した状態でメッセージを送信し、送信先情報処理装置は、送信元情報処理装置の公開鍵を用いて前記電子署名を復号化することによりメッセージを検証することを特徴とするネットワークシステム。

【請求項２】　前記複数の情報処理装置は、その情報処理装置固有の秘密鍵およびその情報処理装置と相互接続している接続先装置の公開鍵を記憶する記憶手段と、接続先装置から、該接続先装置の電子署名の付加されたメッセージを受信する受信手段と、該メッセージを受信したとき、該接続先装置の公開鍵を用いて前記電子署名を復号化する電子署名復号化手段と、復号化により得られたデータ値と、受信したメッセージまたはそのダイジェスト値とを比較することにより、前記メッセージが真正なものであるかどうかを検証する検証手段と、前記メッセージが真正であると判断したとき、前記メッセージまたはそのダイジェスト値を前記秘密鍵により暗号化して電子署名を作成する電子署名作成手段と、該電子署名の付加されたメッセージを、接続先装置から選択されたいずれかの装置に送信する送信手段と、を備えたことを特徴とする請求項１に記載のネットワークシステム。

【請求項３】　第一の情報処理装置に接続されたメッセージ送信者端末をさらに備え、前記複数の情報処理装置のうち少なくとも一つが、前記メッセージ送信者の公開鍵を所有するメッセージ送信者登録装置であり、前記メッセージ送信者端末は、メッセージ送信者から受け付けたメッセージまたはそのダイジェスト値をメッセージ送信者固有の秘密鍵により暗号化して電子署名S_Uを作成する電子署名作成手段と、第一の情報処理装置へ電子署名S_Uを付した前記メッセージを送信する送信手段と、を備え、前記メッセージ送信者登録装置は、メッセージ送信者登録装置固有の秘密鍵、メッセージ送信者の公開鍵および前記メッセージ送信者登録装置と相互接続している接続先装置の公開鍵を記憶する記憶部と、メッセージ送信者端末から直接または他の情報処理装置を介して電子署名S_Uの付加されたメッセージを受け付ける受信手段と、メッセージ送信者の公開鍵を用いて電子署名S_Uを復号化する電子署名復号化手段と、復号化により得られたデータ値と受信したメッセージまたはそのダイジェスト値とを比較することにより前記メッセージが真正なものであるかどうかを検証する検証手段と、前記メッセージが真正であると判断した場合に、前記メッセージまたはそのダイジェスト値をメッセージ送信者登録装置固有の秘密鍵により暗号化してメッセージ送信者登録装置固有の電子署名S_Rを作成する電子署名作成手段と、電子署名S_Rの付加された前記メッセージを他の情報処理装置へ送信する送信手段と、を備えることを特徴とする請求項１または２に記載のネットワークシステム。

【請求項４】　前記メッセージを受信したとき、前記第二の情報処理装置は、相互接続された情報処理装置間のパスを一または二以上経由させて前記ユーザにより指定された情報処理装置に前記メッセージへの応答内容を送付するネットワークシステムであって、相互接続された情報処理装置間のパスにおいて前記応答内容が送信される際、送信元情報処理装置は、送信元情報処理装置固有の秘密鍵により作成した電子署名を付加した状態で前記応答内容を送信し、送信先情報処理装置は、送信元情報処理装置の公開鍵を用いて前記電子署名を復号化することにより前記応答内容を検証することを特徴とする請求項１乃至３のいずれかに記載のネットワークシステム。

【請求項５】　複数の情報処理装置がツリー状に配列された階層構造を有するネットワークシステムを用いた情報送信方法であって、前記階層構造中の第一の情報処理装置がユーザから受け付けたメッセージを、相互接続された情報処理装置間のパスを一または二以上経由させて、前記メッセージに応答する前記階層構造中の第二の情報処理装置へ送信するステップを含み、該ステップを実行する際、送信元情報処理装置は、送信元情報処理装置固有の秘密鍵により作成した電子署名を付加した状態でメッセージを送信し、送信先情報処理装置は、送信元情報処理装置の公開鍵を用いて前記電子署名を復号化することによりメッセージを検証することを特徴とする情報送信方法。

【請求項６】　複数の情報処理装置がツリー状に配列された階層構造を有し、該階層構造中の第一の情報処理装置に接続されたメッセージ送信者端末を備え、該階層構造中に前記メッセージ送信者の公開鍵を所有するメッセージ送信者登録装置を含むネットワークシステムを用いた情報送信方法であって、前記メッセージ送信者端末が、サービス享受者から受け付けた要求またはそのダイジェスト値をメッセージ送信者固有の秘密鍵により暗号化して電子署名S_Uを作成し、次いで、電子署名S_Uを付した前記メッセージを第一の情報処理装置へ送信する第一のステップと、第一の情報処理装置とメッセージ送信者登録装置が異なる場合に、第一の情報処理装置が、メッセージ送信者登録装置へ、電子署名S_Uを付した前記メッセージを転送する第二のステップと、メッセージ送信者登録装置から、相互接続された情報処理装置間のパスを一または二以上経由させて、前記メッセージに応

答する前記階層構造中の第二の情報処理装置へ送信する第三のステップと、を含み、前記第三のステップを実行する際、送信元情報処理装置は、送信元情報処理装置固有の秘密鍵により作成した電子署名を付加した状態でメッセージを送信し、送信先情報処理装置は、送信元情報処理装置の公開鍵を用いて前記電子署名を復号化することによりメッセージを検証することを特徴とする情報送信方法。

【請求項７】　前記メッセージを受信したとき、前記第二の情報処理装置は、相互接続された情報処理装置間のパスを一または二以上経由させて前記ユーザにより指定された情報処理装置に前記メッセージへの応答内容を送付するステップをさらに有し、該ステップを実行する際、送信元情報処理装置は、送信元情報処理装置固有の秘密鍵により作成した電子署名を付加した状態で前記応答内容を送信し、送信先情報処理装置は、送信元情報処理装置の公開鍵を用いて前記電子署名を復号化することにより前記応答内容を検証することを特徴とする請求項５または６に記載の情報送信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子署名を用いた情報送信技術に関するものである。

【０００２】

【従来の技術】近年におけるネットワーク技術の進歩にともない、通信ネットワークを介して様々な情報通信が行われるようになってきた。このような流れの中で、行政サービス機関に対する各種書類申請を電子的に行うためのインフラ整備が進みつつある。

【０００３】一般に、ネットワークを介して情報の授受を行う場合、通信相手の本人確認が難しく、また、送信データが盗用されたり、改ざんされたりする恐れがあり、そのための対策が必要不可欠となる。このような対策の一つとして、電子署名を用いた電子認証方式が広く利用されている。この電子認証方式では、送信者が、秘密鍵により暗号化された電子署名をメッセージに付加して送信し、受信者が、送信者の公開鍵を用いて電子署名を復号化し、メッセージのダイジェスト値と照合する。この方式によれば、送信元の確認および改ざんの有無を確実にチェックすることができる。

【０００４】このような方式を、たとえば行政サービス機関における電子書類申請に適用しようとした場合、行政機関間での電子認証を円滑に行うことが重要な技術的課題となる。この点について以下、説明する。

【０００５】行政機関利用者の申請する書類の発行権限は複数の機関にわたるため、利用者は、書類の種類に応じて様々な行政機関に申請を行う必要がある。このため、利用者が自己の電子署名を付して書類発行権限を有する機関に申請書を送付しようとした場合、自己の公開鍵を、申請先の各機関にそれぞれ登録しておく必要が生じ、登録手続きの労力が多大となる。特に、各行政機関がそれぞれ異なる認証局を使用し、互いに他の行政機関が使用している認証局の証明書を持っていない場合、利用者は、数種類の秘密鍵、公開鍵および電子証明書の組み合わせを認証局に申請し、取得する必要が生じる。鍵、証明書の申請は厳密な本人確認や審査を要することから、このための労力はきわめて多大である。また、取得した鍵等の管理も煩雑となる。行政機関にとっても、多量の公開鍵、証明書を所持する必要が生じ、しかも証明書の有効期限管理等が必要となるため、負担が大きい。

【０００６】行政機関から提供される書類の多くは個人情報を含むものであるため、なりすましや改ざんの防止に関し、特に高い水準のセキュリティが求められる。こうした状況下、高水準のセキュリティを保ちつつ行政機関間での電子認証を円滑に行うための技術が強く望まれている。

【０００７】

【発明が解決しようとする課題】本発明は上記事情に鑑みなされたものであって、電子署名を用いたネットワーク上の情報送信において、管理する鍵の数を低減しつつ、高いセキュリティレベルを実現し、なりすましや改ざん等の不正行為を効果的に防止する技術を提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明によれば、複数の情報処理装置がツリー状に配列された階層構造を有し、該階層構造中の第一の情報処理装置がユーザから受け付けたメッセージを、相互接続された情報処理装置間のパスを一または二以上経由させて、前記メッセージに応答する前記階層構造中の第二の情報処理装置へ送信するネットワークシステムであって、各情報処理装置は、その装置固有の秘密鍵を有し、その装置と直接接続する他の情報処理装置は、前記秘密鍵に対応する公開鍵を有し、相互接続された情報処理装置間のパスにおいてメッセージが送信される際、送信元情報処理装置は、送信元情報処理装置固有の秘密鍵により作成した電子署名を付加した状態でメッセージを送信し、送信先情報処理装置は、送信元情報処理装置の公開鍵を用いて前記電子署名を復号化することによりメッセージを検証することを特徴とするネットワークシステム、が提供される。

【０００９】このネットワークシステムおいて、メッセージは、相互接続された情報処理装置間のパスを経由して、第一の情報処理装置から第二の情報処理装置に送信される。各パスにおいては、そのパスに固有の秘密鍵－公開鍵のペアによる電子認証を行いながらメッセージが送信される。このため、第一の情報処理装置から第二の情報処理装置にメッセージが送信される過程において、各情報処理装置間で逐一電子認証が行われることとなる。この結果、メッセージの検証が確実に行われ、なり

すましやメッセージの改ざんを効果的に防止することができる。

【００１０】また、情報処理装置がツリー状に配列されているため、各情報処理装置は、自己の秘密鍵のほか、直接接続する上位および下位の情報処理装置の公開鍵のみを保有すればすむこととなり、システム全体の鍵保有数を顕著に低減できる。

【００１１】なお、このネットワークシステムにおいては、ツリー構造の頂点に位置する情報処理装置を除く各情報処理装置が、それぞれ単一の親装置を有する構造とすることができる。このようにした場合、システム全体の鍵保有数をより顕著に低減できる。

【００１２】上記ネットワークシステムにおいて、前記複数の情報処理装置は、その情報処理装置固有の秘密鍵およびその情報処理装置と相互接続している接続先装置の公開鍵を記憶する記憶手段と、接続先装置から、該接続先装置の電子署名の付加されたメッセージを受信する受信手段と、該メッセージを受信したとき、該接続先装置の公開鍵を用いて前記電子署名を復号化する電子署名復号化手段と、復号化により得られたデータ値と、受信したメッセージまたはそのダイジェスト値とを比較することにより、前記メッセージが真正なものであるかどうかを検証する検証手段と、前記メッセージが真正であると判断したとき、前記メッセージまたはそのダイジェスト値を前記秘密鍵により暗号化して電子署名を作成する電子署名作成手段と、該電子署名の付加されたメッセージを、接続先装置から選択されたいずれかの装置に送信する送信手段と、を備えた構成とすることができる。このような構成を採用することにより、メッセージの送信過程においてより一層確実に電子認証を行うことができる上、鍵の保有数を確実に低減することができる。

【００１３】また上記ネットワークシステムにおいて、第一の情報処理装置に接続されたメッセージ送信者端末をさらに備え、前記複数の情報処理装置のうち少なくとも一つが、前記メッセージ送信者の公開鍵を所有するメッセージ送信者登録装置であり、前記メッセージ送信者端末は、メッセージ送信者から受け付けたメッセージまたはそのダイジェスト値をメッセージ送信者固有の秘密鍵により暗号化して電子署名S_Uを作成する電子署名作成手段と、第一の情報処理装置へ電子署名S_Uを付した前記メッセージを送信する送信手段と、を備え、前記メッセージ送信者登録装置は、メッセージ送信者登録装置固有の秘密鍵、メッセージ送信者の公開鍵およびメッセージ送信者登録装置と相互接続している接続先装置の公開鍵を記憶する記憶部と、メッセージ送信者端末から直接または他の情報処理装置を介して電子署名S_Uの付加されたメッセージを受け付ける受信手段と、メッセージ送信者の公開鍵を用いて電子署名S_Uを復号化する電子署名復号化手段と、復号化により得られたデータ値と受信したメッセージまたはそのダイジェスト値とを比較することにより前記メッセージが真正なものであるかどうかを検証する検証手段と、前記メッセージが真正であると判断した場合に、前記メッセージまたはそのダイジェスト値をメッセージ送信者登録装置固有の秘密鍵により暗号化してメッセージ送信者登録装置固有の電子署名S_Rを作成する電子署名作成手段と、電子署名S_Rの付加された前記メッセージを他の情報処理装置へ送信する送信手段と、を備えた構成とすることもできる。

【００１４】このネットワークシステムによれば、メッセージ送信者は、自己の端末から、セキュリティを保ちつつ容易にネットワークへメッセージを送信することができる。そして、ネットワークシステムを構成するいずれかの情報処理装置がメッセージ送信者の公開鍵を所有していれば、そのメッセージを目的の場所へ到達させることができる。このため、メッセージ送信者にとっては公開鍵等の登録を一回行うだけで、その後はセキュリティを保ちつつメッセージを送信できることとなり、労力が低減されるという利益が得られる。一方、当該ネットワークシステムにとっては、メッセージ送信者の公開鍵を一つの情報処理装置のみが所有していればよいこととなり、管理する鍵の数を低減できるという利益が得られる。特に、多くのメッセージ送信者をユーザにもつネットワークシステムにおいては、管理する鍵の数の低減効果は絶大である。

【００１５】また、上記ネットワークシステムにおいて、前記メッセージを受信したとき、前記第二の情報処理装置は、相互接続された情報処理装置間のパスを一または二以上経由させて前記ユーザにより指定された情報処理装置に前記メッセージへの応答内容を送付するネットワークシステムであって、相互接続された情報処理装置間のパスにおいて前記応答内容が送信される際、送信元情報処理装置は、送信元情報処理装置固有の秘密鍵により作成した電子署名を付加した状態で前記応答内容を送信し、送信先情報処理装置は、送信元情報処理装置の公開鍵を用いて前記電子署名を復号化することにより前記応答内容を検証する構成を採用することもできる。

【００１６】このような構成を採用した場合、メッセージ送信者は、ネットワークを介して送信したメッセージの応答内容を、ネットワークを通じて取得することができるため、メッセージ送信者にとっては、高いセキュリティが保たれた状態で迅速にメッセージの応答内容を得ることができるという利益があり、一方、ネットワークシステムにとっては、応答内容を迅速に送付できる上、印刷物等の形態で送付する場合に比べてコスト低減効果が得られる場合もある。

【００１７】さらに発明によれば、複数の情報処理装置がツリー状に配列された階層構造を有するネットワークシステムを用いた情報送信方法であって、階層構造中の第一の情報処理装置がユーザから受け付けたメッセージを、相互接続された情報処理装置間のパスを一または二

以上経由させて、メッセージに応答する階層構造中の第二の情報処理装置へ送信するステップを含み、該ステップを実行する際、送信元情報処理装置は、送信元情報処理装置固有の秘密鍵により作成した電子署名を付加した状態でメッセージを送信し、送信先情報処理装置は、送信元情報処理装置の公開鍵を用いて電子署名を復号化することによりメッセージを検証することを特徴とする情報送信方法、が提供される。

【００１８】また発明によれば、複数の情報処理装置がツリー状に配列された階層構造を有し、該階層構造中の少なくとも一つの情報処理装置に接続されたメッセージ送信者端末を備え、該階層構造中にメッセージ送信者の公開鍵を所有するメッセージ送信者登録装置を含むネットワークシステムを用いた情報送信方法であって、メッセージ送信者端末が、サービス享受者から受け付けた要求またはそのダイジェスト値をメッセージ送信者固有の秘密鍵により暗号化して電子署名ＳＵを作成し、次いで、メッセージ送信者端末と接続する第一の情報処理装置へ、作成された電子署名ＳＵを付したメッセージを送信する第一のステップと、第一の情報処理装置とメッセージ送信者登録装置が異なる場合に、第一の情報処理装置が、メッセージ送信者登録装置へ、電子署名ＳＵを付したメッセージを転送する第二のステップと、メッセージ送信者登録装置から、相互接続された情報処理装置間のパスを一または二以上経由させて、メッセージに応答する階層構造中の第二の情報処理装置へ送信する第三のステップと、を含み、第三のステップを実行する際、送信元情報処理装置は、送信元情報処理装置固有の秘密鍵により作成した電子署名を付加した状態でメッセージを送信し、送信先情報処理装置は、送信元情報処理装置の公開鍵を用いて電子署名を復号化することによりメッセージを検証することを特徴とする情報送信方法、が提供される。

【００１９】上記情報送信方法によれば、メッセージは、相互接続された情報処理装置間のパスを経由して、第一の情報処理装置から第二の情報処理装置に送信される。各パスにおいては、そのパスに固有の秘密鍵－公開鍵のペアによる電子認証を行いながらメッセージが送信される。このため、第一の情報処理装置から第二の情報処理装置にメッセージが送信される過程において、各情報処理装置間で逐一電子認証が行われることとなる。この結果、メッセージの検証が確実に行われ、なりすましやメッセージの改ざんを効果的に防止することができる。

【００２０】また、情報処理装置がツリー状に配列されているため、各情報処理装置は、自己の秘密鍵のほか、直接接続する上位および下位の情報処理装置の公開鍵のみを保有すればすむこととなり、システム全体の鍵保有数を顕著に低減できる。

【００２１】上記情報送信方法において、メッセージを受信したとき、第二の情報処理装置は、相互接続された情報処理装置間のパスを一または二以上経由させてユーザにより指定された情報処理装置にメッセージへの応答内容を送付するステップをさらに有し、該ステップを実行する際、送信元情報処理装置は、送信元情報処理装置固有の秘密鍵により作成した電子署名を付加した状態で応答内容を送信し、送信先情報処理装置は、送信元情報処理装置の公開鍵を用いて電子署名を復号化することにより応答内容を検証する構成とすることもできる。

【００２２】このような構成を採用した場合、メッセージ送信者は、ネットワークを介して送信したメッセージの応答内容を、ネットワークを通じて取得することができるため、メッセージ送信者にとっては、高いセキュリティが保たれた状態で、迅速にメッセージの応答内容が得られるという利益があり、一方、ネットワークシステムにとっては、応答内容を迅速に送付できる上、印刷物等の形態で送付する場合に比べてコスト低減効果が得られる場合もある。

【００２３】本発明においては、各情報処理装置と直近の接続先装置との間の情報の送受信が確保されれば、ネットワークシステム中の任意の装置間で情報を伝達できることとなる。したがって、ネットワークシステム中に様々な通信方式が混在してもかまわない。

【００２４】本発明におけるメッセージ送信者端末は、ＩＣカード等の記憶媒体に格納された情報を読み出す媒体読み取り手段を具備し、この記憶媒体からメッセージ送信者の秘密鍵を読み出す方式とすることもできる。

【００２５】なお、上記構成要素の任意の組合せや、本発明の表現を方法、装置、システム、記録媒体、コンピュータプログラムなどの間で変換したものもまた、本発明の態様として有効である。

【００２６】

【発明の実施の形態】図１は、本発明の好ましい実施の形態の一例を示す図である。サービス申請装置１０１はサービス享受者１３０のサービス申請書を発信する装置である。サービス申請装置１０１は、一方向性関数を用いてサービス申請書のメッセージダイジェスト値を算出するとともに、サービス申請装置１０１に接続されたＩＣカード１１０から秘密鍵を読み出し、これを用いて上記メッセージダイジェスト値を暗号化して電子署名ＳＵを作成する。具体的には、例えば、サービス申請書にハッシュ関数演算を行ってハッシュ値を得、これを秘密鍵で暗号化することにより電子署名ＳＵを作成する。

【００２７】サービス申請装置１０１の内部構造を図７に示す。サービス申請装置１０１の本体部４０は、インターフェース４５ｂを介してネットワーク４１と接続し、データの授受を行う。また、インターフェース４５ａを介してリーダライタ４２および外部記憶装置４３と接続し、データの授受を行う。リーダライタ４２はＩＣカードから秘密鍵等の情報を取得する役割を果たす。本

体部４０内部には、本体部４０の全体の動きを制御するＣＰＵ４６、各種のプログラムやデータが格納されたメモリ４８がバスを介して接続されている。メモリは、以下の機能を有する部分を具備している。

（ａ）本体部４０固有の秘密鍵と、相互接続している接続先装置の公開鍵とを記憶する記憶部

（ｂ）メッセージまたはそのダイジェスト値を秘密鍵により暗号化して電子署名ＳＵを作成する電子署名作成部

（ｃ）電子署名付メッセージを受け取ったとき、電子署名を復号化する電子署名復号化部

（ｄ）復号化により得られたデータ値と、受信したメッセージまたはそのダイジェスト値とを比較することにより、メッセージが真正なものであるかどうかを検証する検証部

【００２８】インターフェース４５は、接続先装置から、ユーザからメッセージの入力を受け付けるとともに、サービス申請装置１０１の電子署名ＳＵを付して接続先装置に送信する役割を果たす。

【００２９】図１に戻り、この電子署名ＳＵを付したサービス申請書を登録サーバ１０２に送信する。登録サーバ１０２は、サービス享受者１３０の公開鍵およびその電子証明書があらかじめ登録されたデータベース（不図示）を備えている。登録サーバ１０２において、サービス申請装置１０１から受信した電子署名ＳＵはサービス享受者１３０の公開鍵を用いて復号化され、これとサービス申請書のメッセージダイジェスト値を比較することにより、メッセージ送信元の確認、および、メッセージの改ざんのチェックがなされる。その後、登録サーバ１０２で作成された電子署名ＳＲ付サービス申請書が、登録サーバ１０２から、複数の連絡サーバからなるネットワーク１２０を経由して、サービス提供サーバ１０４へ送信される。

【００３０】サービス提供サーバ１０４は、サービス享受者１３０のサービス申請書を受け、これに対応してサービス享受者１３０にサービスを提供する。サービスの提供については様々な形態を採用することができる。たとえば、ネットワークを利用し、上記した流れを逆にたどってサービスの目的物を電子的に送信してもよいし、サービス提供サーバ１０４からサービス申請書を受け取った者が、サービスの目的物をサービス享受者１３０に直接送付したり、サービス提供者を派遣する等の方式を採用することもできる。なお、ネットワークを利用してサービスの目的物を送信する場合は、サービス申請書の場合と同様、各サーバ間で逐一電子署名による認証を行いながら送信することが望ましい。あるいは、目的物そのものを暗号化して送信する形式としてもよい。

【００３１】上記実施形態では、サービス申請装置１０１は、サービス申請装置１０１に接続されたＩＣカード１１０から秘密鍵を読み出す方式を採用している。したがって、サービス享受者１３０は、予め秘密鍵等の格納されたＩＣカードを作成しておく必要がある。ここで、ＩＣカード作成の手順を図２に示す。まずサービス享受者１３０から認証機関１４０へ、ＩＣカードの申請がなされる（Ｓ５１）。この申請を受けて認証機関１４０は、申請者がサービス享受者１３０本人であることを何らかの方法で確認し、審査の上、ＩＣカードを発行してサービス享受者１３０へ送付する（Ｓ５２）。このＩＣカードには、サービス享受者１３０の公開鍵付き電子証明書が格納されている。サービス享受者１３０はこのＩＣカードを受け取った後、秘密鍵を作成してＩＣカードに格納する（Ｓ５３）。次いでサービス享受者１３０はサービス申請装置１０１に対し、公開鍵、電子証明書の登録を申請する（Ｓ５４）。これを受けてサービス申請装置１０１は、ＩＣカード１１０に接続するデータベース（不図示）にサービス享受者１３０の公開鍵および電子証明書を登録した後（Ｓ５５）、サービス享受者１３０へ完了通知を送付する（Ｓ５６）。以上により、サービス申請装置１０１に対するサービス享受者１３０の情報の登録作業が完了する。なお、ここでは秘密鍵をサービス享受者１３０が自分で作成しているが、認証機関１４０やこれに代わる機関が秘密鍵を作成し、これをＩＣカード１１０に格納する方式とすることもできる。

【００３２】図２におけるＳ５１およびＳ５２のステップについて、図３を参照してより詳細に説明する。図中、点線部分はオフライン、実線部分はオンラインであることを示す。認証機関１４０とＩＣカード１１０の関係については、たとえば、認証機関１４０のパソコン端末にＩＣカード１１０を接続し、このパソコン端末によってＩＣカード１１０を操作する形態とする。

【００３３】図３において、まず、サービス享受者１３０が認証機関１４０へＩＣカードの発行を申し込む（Ｓ６１（図２のＳ５１に対応））。次いで認証機関１４０は、カード発行のための審査を行う（Ｓ６２）。ここで、本人確認が行われるとともに電子証明書等を作成するための個人情報が認証機関１４０に提供される。本人確認は、対面審査またはそれに代わる厳密な確認方法とすることが好ましい。

【００３４】審査をパスした場合、認証機関１４０はＩＣカード１１０に鍵作成指令を送る（Ｓ６３）。これを受けてＩＣカード１１０に内蔵されたプログラムが起動し、公開鍵が作成される（Ｓ６４）。この公開鍵はＩＣカード１１０に格納されるとともに、認証機関１４０に公開鍵が送信される（Ｓ６５）。認証機関１４０はこの公開鍵の証明書を作成した後（Ｓ６６）、これをＩＣカード１１０に送信する（Ｓ６７）。証明書はＩＣカード１１０に格納され（Ｓ６８）、完了通知が認証機関１４０に送信される（Ｓ６９）。以上のようにしてＩＣカード１１０が作成される。このＩＣカード１１０の内部構造を図４に示す。ＣＰＵ１１がカード全体の機能を制御し、このＣＰＵ１１がバスを介して、インターフェース

部１２、鍵作成部１３、電子署名作成部１４およびメモリ１５と接続している。インターフェース部１２は、ＩＣカード１１０が組み込まれる装置とのデータのやりとりを行う部分である。鍵作成部１３は公開鍵を作成する部分である。電子署名作成部１４は、公開鍵を使って電子署名を作成する部分である。メモリ１５は、カード所有者の個人情報やその他のデータ、および、各種プログラムを記憶する部分である。図３に戻って、このような構造のＩＣカードが、認証機関１４０からサービス享受者１３０へ送付される（Ｓ７０）。

【００３５】次に、本発明の他の例について説明する。図１０は本実施形態に係るネットワークシステムの概略構造を示す図である。このネットワークシステムは、双方向リンクにより相互接続された複数のサーバおよび装置がツリー状に配列された階層構造を有している。ツリー構造の頂点に位置する情報処理装置を除く各情報処理装置は、それぞれ単一の親装置を有している。

【００３６】サービス申請装置１０１、登録サーバ１０２および中継サーバ１０３は、いずれも図１１のような内部構造を有している。すなわち、サーバ本体部７０は、インターフェース７５を介してネットワーク７１と接続し、データの授受を行う。本体部７０内部には、本体部７０の全体の動きを制御するＣＰＵ７６、各種のプログラムやデータが格納されたメモリ７８がバスを介して接続されている。

【００３７】メモリ７８は、以下の機能を有する部分を具備している。

（ａ）当該情報処理装置固有の秘密鍵と、相互接続している接続先装置の公開鍵とを記憶する記憶部

（ｂ）データ送信元の装置の公開鍵を用いて電子署名を復号化する電子署名復号化部

（ｃ）電子署名復号化によって得られるデータ値と、受信した情報またはそのダイジェスト値とを、比較することにより、受け取った情報が真正なものであるかどうかを検証する検証部

（ｄ）上記情報が真正であると判断した場合に、上記情報またはそのダイジェスト値を秘密鍵により暗号化して電子署名を作成する電子署名作成部

【００３８】インターフェース７５は、接続先装置から、接続先装置の電子署名が付加された情報を受信するとともに、本体部７０の電子署名を付していずれかの接続先装置に送信する役割を果たす。

【００３９】次に、図１０、図１１に示す構造を備えたネットワークシステムを用いて本発明に係る方法について説明する。図５および図８は、ＩＣカード１１０で受け付けたサービス享受者１３０のサービス申請書が、登録サーバ１０２および中継サーバ１０３ａ～ｅを介してサービス提供サーバ１０４に送信され（図５、Ｓ１２ａ～Ｓ１２ｆ）、この申請を受けたサービス提供サーバ１０４が、登録サーバ１０２および中継サーバ１０３ａ～ｅを介してサービス申請装置１０１へサービスの目的物を電子的に送付する（図８、Ｓ１３ａ～Ｓ１３ｆ）までの流れを示す。この実施形態では、サービス申請とサービス享受を、同一のサービス申請装置１０１で行っている。

【００４０】図５において、まず、サービス申請装置１０１から登録サーバ１０２へサービス申請書が送信される（Ｓ１１）。このとき、サービス享受者１３０の所有する秘密鍵がＩＣカード１１０から読み出され、これを用いてサービス申請書に電子署名がなされる。この電子署名に基づいてサービス申請装置１０１と登録サーバ１０２の間の認証が行われる。登録サーバ１０２には、サービス享受者１３０の登録鍵およびその電子証明書が予め登録されている。登録サーバ１０２は、サービス申請装置１０１から受信したメッセージが真正なものかどうかを確認するとともに、電子証明書を確認してサービス享受者１３０の登録鍵（公開鍵）が正当なものかどうかを判断する。

【００４１】ここで、電子署名による認証方式について、上記メッセージの確認手順を例に挙げ、図６を参照して説明する。送信元の装置Ａでは、メッセージの平文３１からハッシュ値３２ａが作成され、これが装置Ａ固有の秘密鍵によって暗号化される。この結果、電子署名３３が作成される。装置ＡからＢへは、平文３１とともに電子署名３３が送信される。これを受け取った装置Ｂは、電子署名３３を装置Ａから予め配布された公開鍵を用いて復号化し、ハッシュ値３２ｂを得る。これを、平文３１に基づいて作成したハッシュ値３２ｃと照合する。両者が一致すれば、送信元がＡであることを確認し、かつ、送られた平文３１が改ざんのない真正な文書であることが確認できる。サービス享受者１３０の公開鍵の正当性を確認する際にも、上記と同様の方式が採用される。すなわち、暗号化した電子証明書のダイジェストと、電子証明書の平文をもとに登録サーバ１０２が自ら作成した電子証明書のダイジェストとを比較することにより、電子証明書の信頼性を確認し、公開鍵の正当性を確認することができる。以上述べた方式で、図５におけるサービス申請装置１０１と登録サーバ１０２の間の電子認証が行われる。

【００４２】つづいて、登録サーバ１０２から、中継サーバ１０３を経由してサービス提供サーバ１０４へ、サービス申請書が送信される。送信の過程において、各サーバ間では、それぞれ固有の非対称鍵により作成された電子署名がサービス申請書に付加され、図６で説明した方式による電子認証が逐一行われる。こうして、サービス提供サーバ１０４はサービス申請書を受信する。

【００４３】サービス提供サーバ１０４は、サービス申請書を受信すると、これに対する応答内容をサービス享受者１３０に向けて送信する。このとき、応答内容は、図５の経路を逆にたどってサービス申請装置１０１へ送

信される（図８）。送信の過程において、各サーバ間では、それぞれ固有の非対称鍵により作成された電子署名がサービス申請書に付加され、図６で説明した方式による電子認証が逐一行われる。

【００４４】次に、本発明の他の例について図９を参照して説明する。この例では、図５と類似の方式によってサービス申請書が送信されるが、ユーザ端末であるサービス申請装置２０１から電子署名付きサービス申請を受け付けるサーバと、ユーザの公開鍵や電子証明書が登録されたサーバとが相違する点で図５の場合と異なっている。サービス受付サーバ２０２および中継サーバ２０３は、ユーザの公開鍵や電子証明書を所有していないため、ユーザの電子署名を復号化できず、また、電子証明書に確認によりユーザの公開鍵が正当なものかどうかを判断することができない。このため、この例では、ユーザの電子署名付きサービス申請書は、いったん登録サーバ２０５へ転送される（Ｓ２２ａ～ｆ）。なお、サービス受付サーバ２０２から登録サーバ２０５への転送過程では、各情報処理装置間のパスを経由する際、そのパスに固有の非対称鍵による署名を用い、逐一、電子認証を行うことが望ましい。

【００４５】サービス申請書が登録サーバ２０５に転送されると、ここでユーザの電子署名が復号化され、認証が行われる。その後は図５と同様の手順により中継サーバ２０３間のパスにおける送信が順次行われ、サービス提供サーバ２０６にサービス申請書が到達する（Ｓ２２ｇ～ｌ）。

【００４６】以上、本発明の実施形態について述べたが、以下、より具体的な応用例について説明する。

【００４７】（応用例１）

【００４８】本応用例では、図５および図８と同様の構造のネットワークシステムを用いる。図５および図８におけるランク１、２、３、４を、それぞれ、国、都道府県、市、町のレベルに対応させる。

【００４９】以下、北海道札幌市中央区に本籍を持つ個人Ａが、電子署名登録した千葉県千葉市若葉区にて、戸籍抄本の発行依頼を行う例について説明する。Ａは、サービス申請に先駆け、電子署名用の秘密鍵及び公開鍵の作成、作成した公開鍵の登録サーバへの登録、自分の作成した公開鍵の電子証明書（認証局の公開鍵付き）の発行申請を行い、さらに、作成した自分の秘密鍵や発行された電子証明書等をＩＣカード等の記憶媒体へ格納しておくとともに、電子証明書を登録サーバに登録しておく。

【００５０】以上の準備が終了した段階で、Ａは、図５におけるサービス申請装置１０１を通じて登録サーバ１０２へ、電子化された戸籍抄本の発行依頼書を送信する。依頼書に付随する電子証明書の確認（申請者の公開鍵の確認）は、登録サーバ１０２内で確認することができる。

【００５１】この例では、戸籍抄本発行権限は札幌市中央区のサーバにある。したがって、申請書は、最終的に中央区のサーバに送信される必要がある。ところが、若葉区のサーバが、若葉区の署名付き申請書を直接、札幌市中央区のサーバに送信すると、札幌市中央区のサーバは若葉区のサーバの公開鍵や電子証明書を持っていないので、申請書や公開鍵の真偽の確認をすることができない。そのため、本例では以下の手順により依頼書を送信する。まず、若葉区のサーバが電子署名付き依頼書を、上位の千葉市のサーバに送信し、千葉市サーバは若葉区の電子署名を確認した後、今度は自己の電子署名を付して千葉県のサーバに転送する。同様の手順により、申請書が、千葉県から日本国、日本国から北海道、北海道から札幌市、札幌市から中央区へと依頼書の真偽を確認しながら転送される。そして、札幌市中央区のサーバが依頼書を受け取った後、戸籍抄本が発行される。この戸籍抄本は、申請書が送信されてきたルートを逆方向に進みながら送信される。最終的に、申請場所の若葉区の電子署名が付与されて戸籍抄本が発行される。

【００５２】（応用例２）

【００５３】本応用例では、図９と同様の構造のネットワークシステムを用いる。図９におけるランク１、２、３、４を、それぞれ、国、県、市、町のレベルに対応させる。

【００５４】以下、北海道札幌市中央区に本籍を持つ個人Ａが、出張先の大阪府高石市で戸籍抄本の発行依頼を行う例について説明する。図９におけるサービス受付サーバ２０２が大阪府高石市のサーバ、登録サーバ２０５が千葉市若葉区のサーバ、サービス提供サーバ２０６が札幌市中央区のサーバに、それぞれ該当する。

【００５５】Ａは、千葉県千葉市若葉区に、自己の公開鍵および電子証明書を登録している。この例では、Ａの公開鍵や電子証明書をもたない高石市のサーバがＡの電子署名付き依頼書を受け付けることとなるが、高石市のサーバは、Ａの署名を復号化できず、公開鍵の正当性の確認を行うこともできない。そこで、この依頼書を、高石市から大阪府、日本国、千葉県、千葉市を経由し、若葉区のサーバへ転送する。若葉区のサーバは、このサーバにあらかじめ登録されたＡの公開鍵を用いてＡの署名を復号化し、認証を行う。また、電子証明書の確認により公開鍵の正当性を判断する。その後は応用例１と同様の手順により、戸籍抄本発行権限のある札幌市中央区のサーバに依頼書が送信される。札幌市中央区のサーバが依頼書を受け取った後、戸籍抄本が発行される。この戸籍抄本は、申請書が送信されてきたルートを逆方向に進みながら送信される。最終的に、申請場所の若葉区の電子署名が付与されて戸籍抄本が発行される。

【００５６】上記の応用例のほか、本発明の適用として、たとえば以下のような適用例がある。

【００５７】（適用例１）

15

【００５８】千葉市若葉区に住んでいる個人Ｂが、自分のパソコンで選挙の電子投票を行う。選挙管理センターのサイトにログイン時、自分の電子署名を登録した記憶媒体により有権者本人であるか確認し、電子署名を付与して投票する。

【００５９】（適用例２）

【００６０】千葉市若葉区に住んでいた個人Ｃが、転勤先である徳島県新居浜市で住所変更を行う。Ｃは、千葉県千葉市若葉区に、自己の公開鍵、電子証明書等を登録している。選挙等今後の公民権を行使するため、電子署名の登録先を変更する必要がある。

【００６１】その他、本発明を、不動産登記簿の閲覧、会社の登記、登記情報閲覧等に適用することができる。

【００６２】以上、本発明を実施の形態をもとに説明した。この実施の形態は例示であり、それらの各構成要素や各処理プロセスの組合せにいろいろな変形例が可能なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。

【００６３】

【発明の効果】以上説明したように発明によれば、電子署名を用いたネットワーク上の情報送信において、管理する鍵の数を低減しつつ、高いセキュリティレベルが実現され、なりすましや改ざん等の不正行為を効果的に防止される。

【図面の簡単な説明】

【図１】本発明に係るネットワークシステムの概要を示す図である。

【図２】登録サーバへの電子鍵、電子証明書の登録手順を説明するための図である。

【図３】ＩＣカードの発行手順を説明するための図である。

【図４】ＩＣカードの内部構造を示す図である。

【図５】本発明に係る情報送信を説明するための図である。

【図６】電子署名による認証方法を説明するための図である。

【図７】メッセージ送信者端末の内部構造を示す図である。

【図８】本発明に係る情報送信方法を説明するための図である。

16

【図９】本発明に係る情報送信方法を説明するための図である。

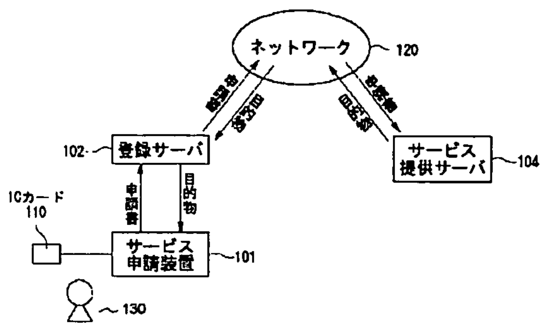
【図１０】本発明に係るネットワークシステムの概要を示す図である。

【図１１】本発明に係るネットワークシステムの概要を示す図である。

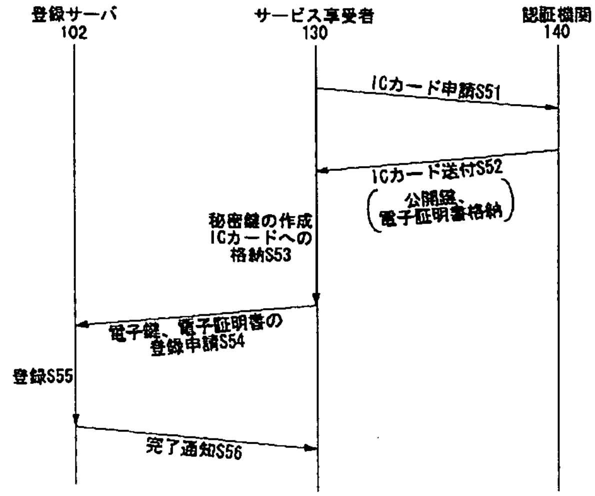
【符号の説明】

１１　ＣＰＵ
１２　インターフェース部
１３　鍵作成部
１４　電子署名作成部
１５　メモリ
３１　平文
３２ａ～ｃ　ハッシュ値
３３　電子署名
４０　本体部
４１　ネットワーク
４２　リーダライタ
４３　外部記憶装置
４５ａ～ｂ　インターフェース
４６　ＣＰＵ
４８　メモリ
７０　本体部
７１　ネットワーク
７５　インターフェース
７６　ＣＰＵ
７８　メモリ
１０１　サービス申請装置
１０２　登録サーバ
１０３ａ～ｅ　中継サーバ
１０４　サービス提供サーバ
１１０　ＩＣカード
１２０　ネットワーク
１３０　サービス享受者
１４０　認証機関
２０１　サービス申請装置
２０２　サービス受付サーバ
２０３ａ～ｊ　中継サーバ
２０５　登録サーバ
２０６　サービス提供サーバ

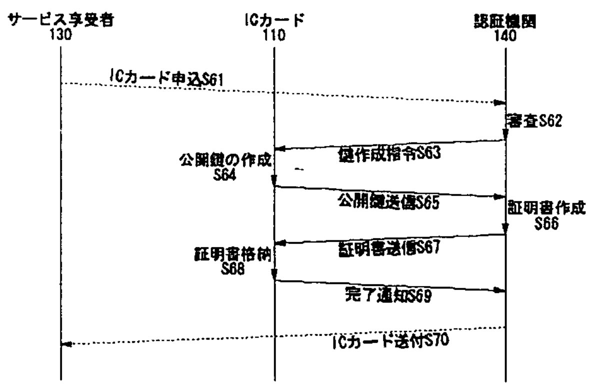
【図１】


ネットワーク
120
102
登録サーバ
サービス
提供サーバ
104
申請書
目的物
ICカード
110
サービス
申請装置
101
130

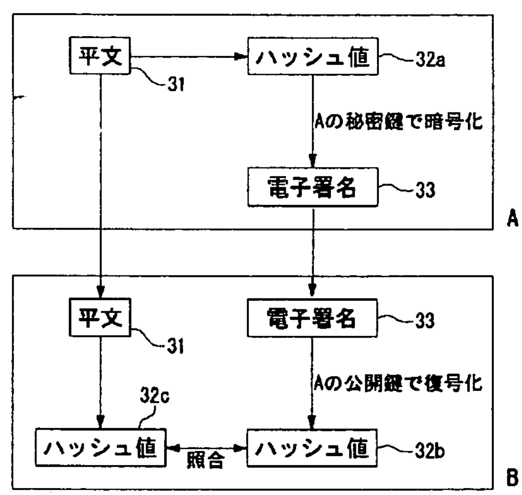
【図２】


登録サーバ
102
サービス享受者
130
認証機関
140
ICカード申請S51
ICカード送付S52
公開鍵、
電子証明書格納
秘密鍵の作成
ICカードへの
格納S53
電子鍵、電子証明書の
登録申請S54
登録S55
完了通知S56

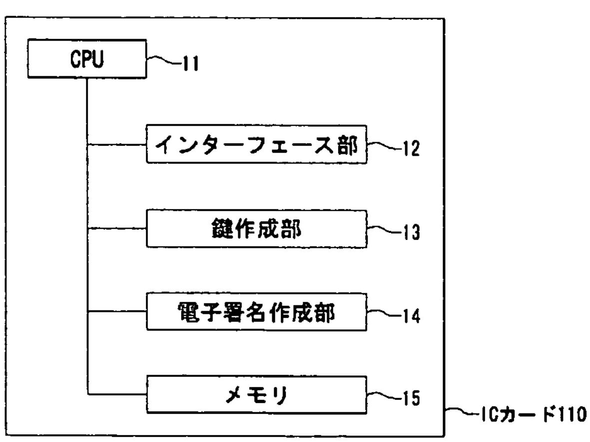
【図３】


サービス享受者
130
ICカード
110
認証機関
140
ICカード申込S61
審査S62
鍵作成指令S63
公開鍵の作成
S64
公開鍵送信S65
証明書作成
S66
証明書送信S67
証明書格納
S68
完了通知S69
ICカード送付S70

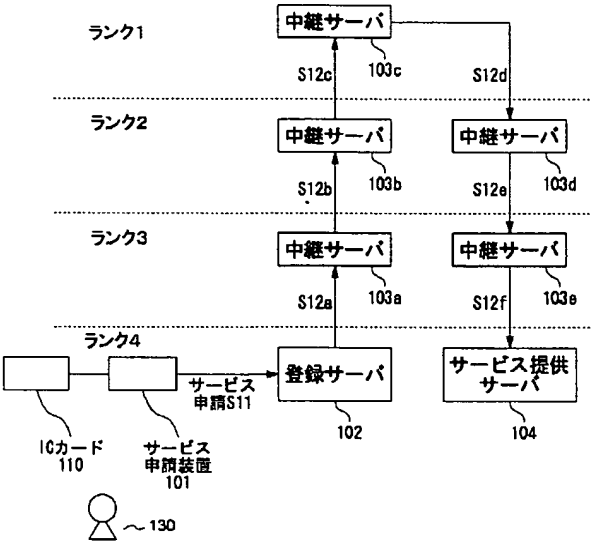
【図６】


平文
31
ハッシュ値
32a
Aの秘密鍵で暗号化
電子署名
33
A
平文
31
電子署名
33
Aの公開鍵で復号化
32c
ハッシュ値
照合
ハッシュ値
32b
B

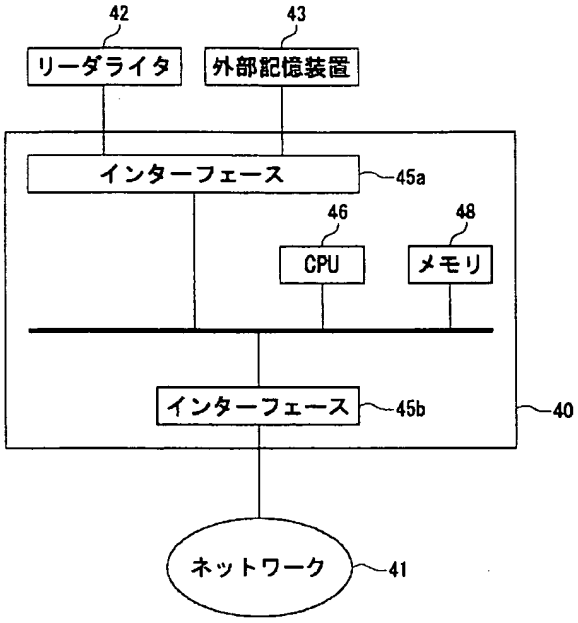
【図４】


CPU
11
インターフェース部
12
鍵作成部
13
電子署名作成部
14
メモリ
15
ICカード110

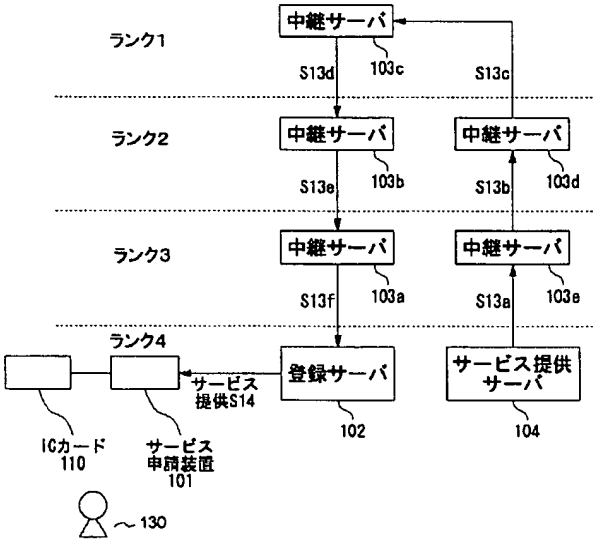
【図５】


ランク1
ランク2
ランク3
ランク4
中継サーバ
103c
S12c
S12d
中継サーバ
103b
中継サーバ
103d
S12b
S12e
中継サーバ
103a
中継サーバ
103e
S12a
S12f
登録サーバ
102
サービス提供サーバ
104
サービス申請S11
ICカード110
サービス申請装置101
130

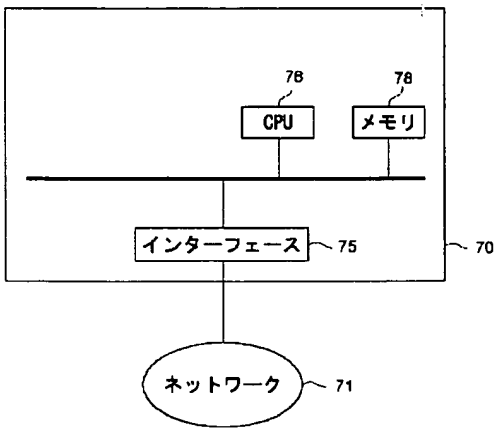
【図７】


42
43
リーダライタ
外部記憶装置
インターフェース
45a
46
48
CPU
メモリ
インターフェース
45b
40
ネットワーク
41

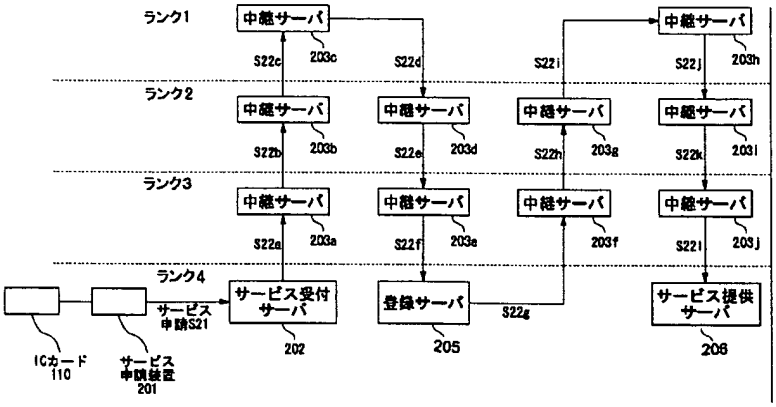
【図８】


ランク1
ランク2
ランク3
ランク4
中継サーバ
103c
S13d
S13c
中継サーバ
103b
中継サーバ
103d
S13e
S13b
中継サーバ
103a
中継サーバ
103e
S13f
S13a
登録サーバ
102
サービス提供サーバ
104
サービス提供S14
ICカード110
サービス申請装置101
130

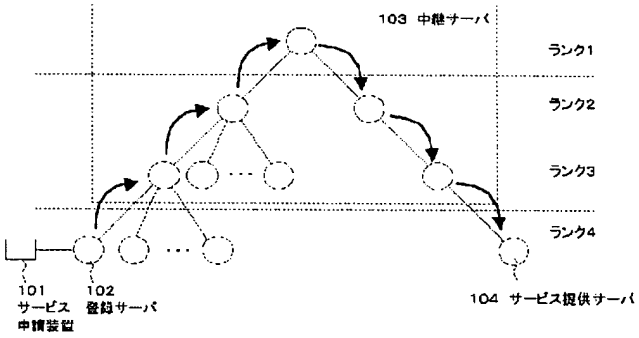
【図１１】


78
78
CPU
メモリ
インターフェース
75
70
ネットワーク
71

【図９】


ランク1
ランク2
ランク3
ランク4
中継サーバ
サービス受付サーバ
登録サーバ
サービス提供サーバ
S22a
S22b
S22c
S22d
S22e
S22f
S22g
S22h
S22i
S22j
S22k
S22l
203a
203b
203c
203d
203e
203f
203g
203h
203i
203j
サービス申請S21
ICカード 110
サービス申請装置 201
202
205
206

【図１０】


103 中継サーバ
ランク1
ランク2
ランク3
ランク4
101 サービス申請装置
102 登録サーバ
104 サービス提供サーバ